PERSONVERNNEMNDA

Org.nr: 986 186 999
E-post: pvn@sivilrett.no
Telefon: 22 99 13 25
sivilrett.no/personvernnemnda

Postadresse:
Postboks 2105 Vika
0125 Oslo

Vår dato:
17.11.2025

Deres dato:

**Unntatt offentlighet**
**Offl. § 13, jf. popplyl. § 24 (1) og fvl. § 13**

Vår referanse:
25/12283

Deres referanse:

# Vedtak i sak PVN-2025-30

**Klage på Datatilsynets vedtak om ileggelse av overtredelsesgebyr for manglende overholdelse av 72-timersfristen for å melde om brudd på personopplysningssikkerheten**

Datatilsynets referanse: 21/03126-13 og -20

## 1. Innledning

Saken gjelder klage fra X Inc. på Datatilsynets vedtak 8. mars 2023 om ileggelse av overtredelsesgebyr for manglende overholdelse av 72-timersfristen for å melde om brudd på personopplysningssikkerheten, jf. personvernforordningen artikkel 33 nr. 1.

Overtredelsesgebyret ble opprinnelig satt til 2 500 000 kroner. I omgjøringsvedtak 2. april 2025 reduserte Datatilsynet gebyret til 1 500 000 kroner på grunn av lang saksbehandlingstid.

## 2. Sakens bakgrunn

Det amerikanske selskapet X Inc. (X) meldte om brudd på personopplysningssikkerheten til Datatilsynet 24. september 2021, jf. personvernforordningen artikkel 33 nr. 1.

Avviksmeldingen ble sendt etter at selskapet 14. juni 2021 oppdaget et datainnbrudd som selskapet var utsatt for mellom 21. mai og 14. juni 2021. X opplyste at en trusselaktør hadde fått uautorisert tilgang til e-postkassen til "X's US Senior Vice President of Human Resources". I avviksmeldingen til Datatilsynet 24. september 2021 beskrev X bruddet på personopplysningssikkerheten slik i pkt. 1.4:

> "In addition to the Mailbox Rules created by the Threat Actor, further investigation, using a PowerShell script, and completed by X and its cyber forensic expert on 19 July 2021, revealed that two files within the One Drive connected to the Mailbox Account (the "**Share Files**") were accessed by the Threat Actor, as detailed in the One Drive logs. These Share Files included (i) a spreadsheet containing the salary and benefits personal data of all 20 of X's European employees (including 16 employee located in EU/UK jurisdictions, as explored at paragraph 2 below), and (ii) a template spreadsheet in the format of (i) that did not contain any personal data."

Trusselaktøren fikk altså tilgang til et regneark som inneholdt personopplysninger om Xs 20 ansatte i Europa. Én av de ansatte arbeidet i Norge.

Datatilsynet ba X om å redegjøre for avviket 4. oktober 2021. X ga slik redegjørelse 28. oktober 2021.

Datatilsynet varslet X 31. januar 2022 om at tilsynet ville ilegge selskapet et overtredelsesgebyr på 2 500 000 kroner for brudd på meldefristen i personvernforordningen artikkel 33. Datatilsynet la til grunn at X fikk kjennskap til bruddet på personopplysningssikkerheten iallfall 19. juli 2021, og at avviksmeldingen ble sendt til Datatilsynet først 67 kalenderdager etter denne datoen.

X ga sine merknader til varselet 22. februar og 11. mars 2022.

Datatilsynet la til grunn at avviksmeldingen ble sendt betydelig etter utløpet av 72 timers-fristen i personvernforordningen artikkel 33 nr. 1, og fattet derfor vedtak 8. mars 2023 om ileggelse av overtredelsesgebyr på 2 500 000 kroner for brudd på meldefristen. Vedtaket har slik slutning:

> "Pursuant to Articles 58(2)(i) and 83(4)(a) GDPR, we impose an administrative fine of NOK 2 500 000 (two million and five hundred thousand) against X, Inc. for:
>
> - having infringed Article 33(1) GDPR by failing to notify a personal data breach without undue delay."

Datatilsynet la til grunn at X hadde mangelfulle rutiner for å sikre rettidig innsending av avviksmelding. Det ble ikke lagt til grunn at det var mangler ved personopplysningssikkerheten.

X påklaget Datatilsynets vedtak 29. mars 2023. Klagen gjelder både grunnlaget for overtredelsesgebyret og sanksjonsfastsettelsen.

Datatilsynet behandlet klagen 2. april 2025. Tilsynet opprettholdt gebyrileggelsen og mente at det på vedtakstidspunktet var grunnlag for å utmåle et overtredelsesgebyr på 2 500 000 kroner. Datatilsynet reduserte imidlertid gebyrets størrelse med 1 000 000 kroner på grunn av lang saksbehandlingstid, slik at overtredelsesgebyret ble satt til 1 500 000 kroner.

Saken ble oversendt til Personvernnemnda ved brev 2. april 2025. X ble orientert om saken i brev fra nemnda og fikk anledning til å komme med kommentarer. Selskapet ga sine merknader på engelsk i brev til nemnda 23. mai 2025. Etter anmodning fra nemnda sendte X inn en norsk oversettelse av merknadene 26. mai 2025.

Saken ble behandlet i nemndas møter 22. september, 27. oktober og 17. november 2025. Personvernnemnda hadde følgende sammensetning: Marius Stub (leder), Ruth Louise Osborg (nestleder), Morten Goodwin, Marit Kristin Larsen Haarr, Malgorzata Agnieszka Cyndecka, Heri Ramampiaro og Bjørn Aslak Juliussen. Fra nemndas sekretariat var fagdirektør Anette Klem Funderud og førstekonsulent Soz Abdul-Rahman til stede.

### 3. X Inc.'s syn på saken i korte trekk

X gjør gjeldende at det ikke er grunnlag for å ilegge overtredelsesgebyr. Subsidiært anføres det at gebyret er uforholdsmessig høyt, jf. personvernforordningen artikkel 83 nr. 1, og at Datatilsynets vedtak uansett er ugyldig.

Datatilsynet tolker personvernforordningen artikkel 33 nr. 1 feil. X sendte avviksmelding til Datatilsynet «uten ugrunnet opphold» og innen fristen på 72 timer. Det må være adgang til å undersøke arten og omfanget av datainnbruddet før varsel sendes. Plikten til å varsle kan iallfall ikke begynne å løpe før det er avklart om datainnbruddet omfattes av forordningen.

Det var først 21. september 2021 at det ble avklart at datainnbruddet bl.a. hadde gitt tilgang til personopplysninger om én person i Norge, og at det ikke var usannsynlig at hendelsen kunne medføre en risiko for vedkommendes rettigheter og friheter. Varslingsfristen begynte dermed å løpe 21. september 2021, som er tre dager før X meldte om bruddet til Datatilsynet 24. september 2021. Varslingsfristen på 72 timer er dermed overholdt.

Uansett mener X at det ikke foreligger grunnlag for å ilegge overtredelsesgebyr, ettersom bruddet var begrenset og uten konsekvenser for den berørte. Alle berørte personer, inkludert den norske registrerte, ble informert om hendelsen 20. oktober 2021. De mottok all relevant informasjon for å redusere eventuell risiko, og ble tilbudt kredittovervåking i 12 måneder. X er derfor lite å bebreide.

X bestrider Datatilsynets risikobaserte tilnærming ved ileggelsen av overtredelsesgebyr. Et eventuelt brudd på meldeplikten har ikke skapt noen risiko for den registrertes rettigheter og friheter.

Datatilsynet viser til alle registrerte i Europa, men har kun kompetanse i Norge. Tar man utgangspunkt i arten og omfanget av krenkelsen overfor den ene personen som ble berørt, står ikke overtredelsesgebyret i rimelig forhold til overtredelsen. Datainnbruddet omfattet arbeidsrelaterte personopplysninger, herunder opplysninger som navn, stilling, arbeidssted, ansettelsesdato, ferie, lønn, bonus, pensjon og firmabil. Dette er opplysninger som ikke krever en høy grad av beskyttelse.

Datatilsynets vedtak om gebyr bryter også med prinsippet om harmonisert og konsistent håndheving av forordningen i EU/EØS. Tilsvarende saker ble avsluttet av andre europeiske tilsynsmyndigheter i perioden 13. oktober 2021 til 10. mars 2023.

Videre er vedtaket i strid med prinsippet om likebehandling, og det er ikke i samsvar med praksis fra Datatilsynet og Personvernnemnda. Det vises til sak 20/02137-2 og 20/03500-8 fra Datatilsynet, samt PVN-2022-13 fra Personvernnemnda, hvor reaksjonene var mildere til tross for at sakene var mer alvorlige. Sammenlignet med disse sakene fremstår det gebyret som X er ilagt, urimelig høyt.

Med henvisning til sakens alvorlighetsgrad, graden av skyld og antall berørte må det ilagte gebyret, som nå er redusert til 1 500 000 kroner som følge av lang saksbehandlingstid, anses for å være uforholdsmessig etter artikkel 83 nr. 1. Opprettholdes vedtaket, vil det avskrekke behandlingsansvarlige fra nødvendige undersøkelser i etterkant av et datainnbrudd, og føre til innsendelse av premature varsler.

Datatilsynets totale saksbehandlingstid på to år og sju måneder tilsier uansett at gebyret bør bortfalle i sin helhet. Det vises til PVN-2021-13, hvor saksbehandlingstiden var tre år og seks måneder, og PVN-2021-09, hvor den totale saksbehandlingstiden var litt over to år. Dette tilsier at gebyret mot X må frafalles helt.

## 4. Personvernnemndas vurdering

### 4.1 Innledning

Saken gjelder spørsmål om X har brutt 72-timersfristen for å melde inn brudd på personopplysningssikkerheten til Datatilsynet, jf. personvernforordningen artikkel 33. Dersom meldefristen er brutt, oppstår det videre spørsmål om det skal ilegges et overtredelsesgebyr, og hvor stort gebyret i tilfelle skal være, jf. artikkel 83.

### 4.2 Datatilsynets og Personvernnemndas kompetanse

X er et amerikansk selskap med europeisk hovedkontor i Sveits og ansatte i 16 EU-/EØS-land. Én av de ansatte arbeidet i Norge. Nemnda legger i likhet med Datatilsynet til grunn at X er etablert i EØS-

området, jf. personvernforordningen artikkel 3 nr. 1. Etter EU-domstolens dom i sak C-230/14 *Weltimmo* avsnitt 76 er det lagt til grunn at kravet til etablering er oppfylt dersom det foreligger "any real and effective activity – even a minimal one – exercised through stable arrangements". I Personvernrådets retningslinjer 3/2018 "on the territorial scope of the GDPR (Article 3)" side 6 legges det i tråd med dette til grunn at tilstedeværelse av en enkeltansatt kan utgjøre en etablering.

Nemnda legger til grunn at Xs behandling av personopplysninger om den norske ansatte utgjør behandling av personopplysninger som reguleres av personopplysningsloven og personvernforordningen. Dette er for øvrig ikke bestridt i klagen. Datatilsynets kompetanse følger da av personopplysningsloven § 20. Personvernnemndas kompetanse som klageorgan følger av personopplysningsloven § 22.

### 4.3 Foreligger det brudd på meldeplikten?

#### 4.3.1 Rettslige utgangspunkter

Personvernforordningen artikkel 33 gir regler om meldeplikt til tilsynsmyndigheten ved brudd på personopplysningssikkerheten. Artikkel 33 nr. 1 lyder slik:

> «1. Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet i samsvar med artikkel 55, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til tilsynsmyndigheten innen 72 timer, skal årsakene til forsinkelsen oppgis.»

I forordningen artikkel 4 nr. 12 er «brudd på personopplysningssikkerhet» definert som:

> «et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet».

Bestemmelsen må ses i sammenheng med fortalepunkt 87, hvor det uttales:

> «Det bør undersøkes om alle egnede teknologiske sikkerhetstiltak og organisatoriske tiltak er blitt gjennomført for omgående å kunne fastslå om det har funnet sted et brudd på personopplysningssikkerheten, og for omgående å underrette tilsynsmyndigheten og den registrerte. Det bør fastslås om meldingen ble gitt uten ugrunnet opphold, idet det tas særlig hensyn til arten og alvorlighetsgraden av bruddet på personopplysningssikkerheten og konsekvensene og skadevirkningene det har for den registrerte. En slik melding kan føre til inngripen fra tilsynsmyndigheten i samsvar med dens oppgaver og myndighet fastsatt i denne forordning.»

Selv om fortalepunktene ikke er rettslig bindende, gir de bidrag til tolkingen av den bindende del av rettsakten, jf. Torje Sunde, Jon Lunde og Ida Sørebø, *EØS-lovgivningen. Fra EU-rett til EØS-rett og norsk rett*, Universitetsforlaget 2023 side 174.

I denne saken er det på det rene at det foreligger et «brudd på personopplysningssikkerheten». Det følger da av artikkel 33 nr. 1 at det skal gis melding om sikkerhetsbruddet «uten ugrunnet opphold» og «når det er mulig, senest 72 timer etter å ha fått kjennskap til det». Meldeplikten gjelder imidlertid ikke i tilfeller hvor bruddet «sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter». Bestemmelsen reiser flere tolkingsspørsmål.

### 4.3.2 Kravet om varsel «uten ugrunnet opphold»

Når det gjelder kravet om at melding skal gis «uten ugrunnet opphold», bemerker nemnda at forordningen ikke krever at melding skal gis umiddelbart. Rett nok står det i fortalepunkt 87 at varsel skal gis «omgående», men det fremgår allerede av neste setning at det avgjørende er om «meldingen ble gitt uten ugrunnet opphold». På den annen side kan man ikke vente lenger med å gi melding enn det er grunn til.

Nemnda antar at det må bero på en konkret vurdering hvor lenge det er adgang til å vente. Dette har ikke bare støtte i ordlyden («ugrunnet»), som klart forutsetter at det må foretas en konkret vurdering, men også av fortalepunkt 87, hvor det fremgår at det ved vurderingen skal «tas særlig hensyn til arten og alvorlighetsgraden av bruddet på personopplysningssikkerheten og konsekvensene og skadevirkningene det har for den registrerte».

Ved vurderingen må det legges en viss vekt på sammenhengen mellom artikkel 33 nr. 1 og 3, hvor det fremgår hva meldingen «skal» inneholde. Den behandlingsansvarlige kan ikke være forpliktet til å melde fra før det er mulig å oppfylle minimumskravene til hva meldingen skal inneholde. Dette innebærer at plikten til å melde fra ikke vil inntre før det har vært mulig å gjennomføre de undersøkelser som er nødvendige for at den behandlingsansvarlige blant annet skal kunne beskrive «[...] arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt» (bokstav a) og «[...] de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten» (bokstav c).

På den annen side går det en grense for hvor omfattende undersøkelser det er nødvendig å gjennomføre før melding gis. Dette følger dels av at minimumskravene i artikkel 33 nr. 3 ikke er spesielt omfattende, og dels av adgangen til å gi trinnvis informasjon etter artikkel 33 nr. 4. Artikkel 33 nr. 4 fastsetter at «[d]ersom og i den grad det ikke er mulig å gi all informasjon samtidig, kan den gis trinnvis uten ytterligere ugrunnet opphold». Den behandlingsansvarlige kan derfor ikke vente med å melde fra til vedkommende har full klarhet i alle forhold knyttet til bruddet på personopplysningssikkerheten.

### 4.3.3 Kravet om varsel innen 72 timer

Varsel skal uansett gis «senest 72 timer etter [at den behandlingsansvarlige har] fått kjennskap til [bruddet på personopplysningssikkerheten]». Dette supplerer kravet om varsel «uten ugrunnet opphold», og bidrar til å sikre at det ikke går for lang tid før tilsynsmyndigheten varsles. Fristen på 72 timer gjelder imidlertid bare «når det er mulig». Nemnda antar at dette unntaket må tolkes strengt, og at det først og fremst tar sikte på tilfeller hvor det foreligger særlige unntakssituasjoner som innebærer at det for tiden ikke er mulig å gi beskjed. I den foreliggende sak er det ikke nødvendig å gå nærmere inn på dette.

Det fremgår av artikkel 33 nr. 1 at 72-timersfristen begynner å løpe på det tidspunktet den behandlingsansvarlige har «fått kjennskap til det». Det er tilstrekkelig at vedkommende har fått kjennskap til bruddet. Det kreves ikke i tillegg at det er avklart at bruddet er meldepliktig, slik X har gjort gjeldende. En slik tolkning har ingen støtte i ordlyden, og ville dessuten svekke bestemmelsens effektivitet. Kravet til «kjennskap» vil for øvrig være oppfylt dersom den behandlingsansvarlige har rimelig grunn til å tro det foreligger et brudd. Det kreves ikke sannsynlighetsovervekt. Et tilsvarende syn er lagt til grunn i Personvernrådets retningslinjer 9/2022 avsnitt 31:

> “31. As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become ‘aware’ of a breach. The EDPB considers that a controller should be regarded as having become ‘aware’ when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.”

Når fristen først har begynt å løpe, skal den behandlingsansvarlige melde fra om bruddet innen 72 timer dersom det viser seg at bruddet «sannsynligvis» vil medføre en «risiko for fysiske personers rettigheter og friheter». Melding skal gis straks dette spørsmålet er avklart. Den behandlingsansvarlige kan derfor ikke vente til utløpet av 72-timersfristen med å melde fra dersom det er mulig å melde fra på et tidligere tidspunkt. Et tilsvarende syn er lagt til grunn i Personvernrådets retningslinjer 01/2021 avsnitt 9:

> “The breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject. Controllers should make this assessment at the time they become aware of the breach. The controller should not wait for a detailed forensic examination and (early) mitigation steps before assessing whether or not the data breach is likely to result in a risk and thus should be notified.”

Et brudd på personopplysningssikkerheten som *ikke* medfører en risiko, er ikke meldepliktig. At 72-timersfristen har begynt å løpe, er derfor ikke ensbetydende med at melding må gis.

Dersom det ikke lykkes å avklare om bruddet er meldepliktig innen fristens utløp, må den behandlingsansvarlige i første omgang selv ta standpunkt til hva som er mest sannsynlig. Dersom vedkommende unnlater å melde fra, gjøres det på egen risiko.

#### 4.3.4 Meldte X bruddet på personopplysningssikkerheten til Datatilsynet rettidig?

X oppdaget den 14. juni 2021 at utenforstående hadde hatt tilgang til e-postkontoen til selskapets HR-leder i perioden 21. mai 2021 til 14. juni 2021. Hendelsen ble rapportert dagen etter til FBI-kontoret for cyberkriminalitet.

På dette tidspunktet antok X at det utelukkende var datasystemene i USA som var rammet, og at dette bare berørte personopplysninger om amerikanske ansatte. Den 1. juli 2021 ble det klart at saken måtte undersøkes ytterligere. Den 19. juli 2021 viste undersøkelser fra eksterne rettstekniske eksperter at personopplysninger knyttet til europeiske ansatte kunne være kompromittert.

X har opplyst at selskapet først 21. september 2021 ble klar over at personopplysninger knyttet til europeiske ansatte var omfattet av datainnbruddet. Den 24. september 2021 ble åtte europeiske tilsynsmyndigheter varslet, inkludert Datatilsynet.

I avviksmeldingen 24. september 2021 opplyser X følgende om hva de innledende undersøkelsene viste:

> “In addition to the Mailbox Rules created by the Threat Actor, further investigation, using a PowerShell script, and completed by X and its cyber forensic expert on 19 July 2027, revealed that two files within the One Drive connected to the Mailbox Account (the "Share Files") were accessed by the Threat Actor, as detailed in the One Drive logs. These Share Files included (i) a spreadsheet containing the salary and benefits personal data of all 20 of X's European employees (including 16 employee located in EU/UK jurisdictions, as explored at paragraph 2

below), and (ii) a template spreadsheet in the format of (i) that did not contain any personal data."

I Xs merknader til Datatilsynets forhåndsvarsel opplyses det at kunnskapstidspunktet var 29. juli 2021. Nemnda legger imidlertid til grunn at selskapet fikk kjennskap til at europeiske ansatte kunne være berørt allerede 19. juli 2021, slik det fremgår av avviksmeldingen. Dette er senere bekreftet overfor Datatilsynet, slik det fremgår av tilsynets vedtak punkt 3.

Nemnda finner det klart at X allerede 19. juli 2021 hadde kjennskap til at selskapet var utsatt for et brudd på personopplysningssikkerheten som kunne medføre en risiko for norske ansattes rettigheter og friheter. At selskapet ventet helt til 24. september 2021 med å melde fra til Datatilsynet, utgjør både et brudd på plikten til å melde fra «uten ugrunnet opphold», og et brudd på plikten til å melde fra innen 72 timer. Det forelå ingen forhold som skulle tilsi at det ikke var «mulig» å melde fra allerede 19. juli 2021.

Nemnda viser til fortalepunkt 87, hvor det som nevnt fremgår at det ved vurderingen skal «tas særlig hensyn til arten og alvorlighetsgraden av bruddet på personopplysningssikkerheten og konsekvensene og skadevirkningene det har for den registrerte». E-postkassen til en HR-ansvarlig i et stort internasjonalt selskap vil ofte kunne inneholde personopplysninger om en rekke ansatte, og dessuten særlige kategorier personopplysninger som helseopplysninger og opplysninger om fagforeningsmedlemskap, jf. artikkel 9. At X ennå ikke hadde mottatt råd fra sine eksterne juridiske rådgivere, gir ikke tilstrekkelig grunn til å vente med å melde fra.

På denne bakgrunn har nemnda kommet til at X har brutt plikten til å gi melding innenfor de tidsfrister som gjelder etter personvernforordningen artikkel 33 nr. 1.

### 4.4 Bør X ilegges overtredelsesgebyr?

#### 4.4.1 Er det grunnlag for å ilegge overtredelsesgebyr?

Etter personopplysningsloven § 26 kan Datatilsynet ilegge overtredelsesgebyr etter personvernforordningen artikkel 83, jf. artikkel 58 nr. 2 bokstav i.

Det fremgår av artikkel 83 nr. 4 bokstav a at det blant annet kan ilegges overtredelsesgebyr ved brudd på den behandlingsansvarliges forpliktelser etter artikkel 33. Ileggelse av gebyr forutsetter at den behandlingsansvarlige har handlet forsettlig eller uaktsomt, jf. EU-domstolens dom 5. desember 2023 i sak C-807/21 (Deutsche Wohnen) avsnitt 75 og dom 5. desember 2023 i sak C-683/21 (Nacionalinis visuomenės sveikatos centras) avsnitt 80.

Ved vurderingen av om det skal ilegges overtredelsesgebyr, skal det tas hensyn til momentene i personvernforordningen artikkel 83 nr. 2 bokstavene a til k. Etter bokstav a skal det blant annet legges vekt på «karakteren, alvorlighetsgraden og varigheten av overtredelsen».

Nemnda er enig med Datatilsynet i at det er grunnlag for å ilegge overtredelsesgebyr i dette tilfellet. Det er tale om en vesentlig oversittelse av meldefristen, og nemnda finner det klart at det var uaktsomt av selskapet å vente i over to måneder med å melde fra. I denne perioden var Datatilsynet avskåret fra å gripe inn i samsvar med dens oppgaver og myndighet fastsatt i personvernforordningen, se fortalepunkt nr. 87. En form for "inngripen" kunne for eksempel tenkes å være ulike pålegg som kunne ha redusert risikoen for skadevirkninger for den registrerte. Bruddet på meldeplikten er derfor alvorlig, selv om datainnbruddet ikke ga tilgang til særlige kategorier av personopplysninger. Allmennpreventive hensyn tilsier etter dette at det bør ilegges overtredelsesgebyr.

### 4.4.2 Utmåling av gebyret

I Datatilsynets vedtak 8. mars 2023 ble overtredelsesgebyret satt til 2 500 000 kroner. I omgjøringsvedtak 2. april 2025 reduserte Datatilsynet gebyrets størrelse med 1 000 000 kroner på grunn av lang saksbehandlingstid, og satte overtredelsesgebyret til 1 500 000 kroner.

X har gjort gjeldende at det ilagte overtredelsesgebyret fremdeles er uforholdsmessig høyt. Det er vist til at bruddet på personopplysningssikkerheten er lite og uten konsekvenser for den berørte. Gebyret uansett må bortfalle på grunn av lang saksbehandlingstid.

Artikkel 83 nr. 1 fastsetter følgende utgangspunkt for utmålingen av gebyrets størrelse:

> «Hver tilsynsmyndighet skal sikre at ilegging av overtredelsesgebyr i henhold til denne artikkel for overtredelser av denne forordning nevnt i nr. 4, 5 og 6 i hvert enkelt tilfelle er virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende.»

Det fremgår av artikkel 83 nr. 4 bokstav a at gebyret for overtredelse av artikkel 33 ikke kan overstige «10 000 000 euro, eller dersom det dreier seg om et foretak, på opptil 2 % av den samlede globale årsomsetningen i forutgående regnskapsår».

Ved utmålingen av gebyret skal det tas «behørig hensyn» til momentene i forordningen artikkel 83 nr. 2 bokstavene a til k. I det følgende vil nemnda knytte noen bemerkninger til enkelte av disse momentene.

Etter bokstav a skal det tas hensyn til «karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd». X ventet i mer enn to måneder med å melde fra etter at selskapet fikk kjennskap til datainnbruddet. Dette utgjør en grov overtredelse av meldeplikten i artikkel 33. På den annen side var det bare én norsk ansatt som ble berørt av bruddet, og det er ikke holdepunkter for å anta at bruddet har påført vedkommende nevneverdige skadevirkninger.

Etter bokstav b skal det tas hensyn til «hvorvidt overtredelsen ble begått forsettlig eller uaktsomt». Det var uaktsomt å vente i over to måneder med å melde fra.

Etter bokstav d skal det tas hensyn til «den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32». Datatilsynet hadde ingen bemerkninger til personopplysningssikkerheten, og nemnda legger derfor til grunn at datasystemene oppfyller kravene i artikkel 25 og 32.

Etter bokstav g skal det tas hensyn til «kategoriene av personopplysninger som er berørt av overtredelsen». Nemnda legger til grunn at datainnbruddet ikke ga tilgang til noen særlige kategorier av personopplysninger, og at det for øvrig var forholdsvis begrenset mengde av personopplysninger som ble berørt.

Når det gjelder den konkrete utmålingen av overtredelsesgebyret, følger det som nevnt av artikkel 83 nr. 1 at overtredelsesgebyret skal utmåles til et beløp som innebærer at sanksjonen er «virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende». Dette gir tilsynsmyndigheten et vidt skjønn ved utmålingen. Det er imidlertid gitt nærmere anvisninger for utmålingen i Personvernrådets retningslinjer 04/2022. I retningslinjene skilles det mellom tre alvorlighetsgrader; “low”, “medium” og “high”. Når den enkelte overtredelse plasseres i en av disse tre kategoriene, gir retningslinjene anvisning på et utgangspunkt (“a harmonised starting point”) for gebyrutmålingen, jf. avsnitt 60:

> "- When calculating the administrative fine for infringements of a **low level of seriousness**, the supervisory authority will determine the starting amount for further calculation at a point between 0 and 10% of the applicable legal maximum.
>
> - When calculating the administrative fine for infringements of a **medium level of seriousness**, the supervisory authority will determine the starting amount for further calculation at a point between 10 and 20% of the applicable legal maximum.
>
> - When calculating the administrative fine infringements of a **high level of seriousness**, the supervisory authority will determine the starting amount for further calculation at a point between 20 and 100% of the applicable legal maximum."

Med dette som utgangspunkt vil den endelige gebyrfastsettelse bero på omstendighetene i den enkelte sak, og på hvilke skjerpende og formildende momenter som gjør seg gjeldende. Selv om Personvernrådets retningslinjer ikke er bindende for medlemsstatene, har nemnda merket seg at det i LB-2024-154313 legges «betydelig vekt» på disse retningslinjene ved prøvingen av gyldigheten av et vedtak om overtredelsesgebyr etter personopplysningsloven. Også nemnda finner det hensiktsmessig å ta utgangspunkt i den fremgangsmåte retningslinjene gir anvisning på.

Etter nemndas syn har den aktuelle overtredelsen samlet sett «lav alvorlighetsgrad», selv om fristoversittelsen var betydelig. Det vises til nemndas drøftelse ovenfor, hvor det blant annet fremheves at bruddet bare rammet én person, at det ikke berørte særlige kategorier personopplysninger og at opplysningene for øvrig var lite sensitive. Dette innebærer at utgangspunktet skal være et sted mellom 0-10 prosent av den øvre rammen for gebyret. I den konkrete saken – etter å ha tatt hensyn til utmålingsmomentene i artikkel 83 nr. 2 – la Datatilsynet til grunn at overtredelsesgebyret i utgangspunktet burde utgjøre 2 500 000 kroner. Nemnda er enig i at dette utgjør et passende nivå. Legger man til grunn at Xs omsetning på verdensbasis var om lag 300 000 000 USD i 2024, utgjør den øvre rammen for gebyret 6 000 000 USD – eller om lag 60 000 000 kroner. Et gebyr på 2 500 000 kroner utgjør om lag 4 prosent av dette beløpet. Dette reflekterer bruddets alvorlighetsgrad.

Datatilsynet reduserte senere overtredelsesgebyret med 1 000 000 kroner på grunn av lang saksbehandlingstid. X har gjort gjeldende at den samlede saksbehandlingstiden i denne saken så lang at overtredelsesgebyret bør bortfalle helt.

Datainnbruddet, som ble oppdaget 14. juni 2021, ble meldt til Datatilsynet 24. september 2021. Datatilsynet ba X redegjøre for saken 4. oktober 2021. X ga slik redegjørelse 28. oktober 2021. Datatilsynet sendte varsel om overtredelsesgebyr 31. januar 2022. X innga sine merknader 22. februar 2022 og 11. mars 2022. Vedtak om overtredelsesgebyr ble først truffet 8. mars 2023, som var om lag halvannet år etter tilsynet mottok avviksmeldingen. Etter X klaget på vedtaket 29. mars 2023, omgjorde Datatilsynet vedtaket om gebyrets størrelse 2. april 2025, og oversendte saken til klagebehandling til Personvernnemnda samme dag, 2. april 2025.

Nemnda kan ikke se at saken kan forsvare en samlet saksbehandlingstid på tre og et halvt år, heller ikke om det tas hensyn til tilsynets ressurssituasjon. Saken er ikke spesielt omfattende, og den har heller ikke reist spesielle tvilsspørsmål av rettslig eller faktisk karakter.

I tillegg til saksbehandlingstiden hos Datatilsynet, må det også tas hensyn til den tid nemnda har brukt på å behandle saken.

Den samlede saksbehandlingstiden overstiger fire år fra X meldte bruddet til Datatilsynet. Saken er derfor ikke er avgjort innen rimelig tid, jf. forvaltningsloven § 11 a første ledd. Det er ingen unnskyldningsgrunn at saksbehandlingstiden har sammenheng med knappe ressurser. Saker om overtredelsesgebyr må uansett prioriteres, jf. Grunnloven § 95 og EMK artikkel 6 nr. 1.

I nemndas praksis finnes det flere eksempler på at et overtredelsesgebyr er redusert som følge av lang saksbehandlingstid, se f.eks. PVN-2021-03, PVN-2021-13, PVN-2021-16, PVN-2022-03, og PVN-2024-19. I enkelte saker har gebyret bortfalt helt.

Etter nemndas syn er det naturlig at saksbehandlingstidens lengde tillegges en viss vekt ved gebyrutmålingen. I straffesaker utgjør lang saksbehandlingstid et formildende moment ved straffutmålingen, jf. straffeloven § 78 første ledd bokstav e. Overtredelsesgebyr er ikke straff i straffelovens forstand, jf. straffeloven § 29. De lovgivningspolitiske hensyn som taler for at lang saksbehandlingstid bør tillegges vekt ved straffutmålingen, gjør seg imidlertid gjeldende også ved utmålingen av overtredelsesgebyr.

I saker om overtredelsesgebyr følger det av EMK artikkel 6 nr. 1 at saken må avgjøres innen rimelig tid ("within reasonable time"). Nemnda minner for ordens skyld om at denne fristen – i motsetning til kravet om avgjørelse «uten grunnet opphold» i forvaltningsloven § 11 a – ikke begynner å løpe allerede fra det tidspunktet saken innledes. Fristen begynner først å løpe fra det tidspunktet den ansvarlige ble anklaget i konvensjonens forstand. I gebyrsammenheng vil den ansvarlige regnes som anklaget fra det tidspunkt vedkommende mottar et forhåndsvarsel om ileggelse av overtredelsesgebyr. Saken må deretter avgjøres innen rimelig tid. En eventuell krenkelse vil først foreligge når denne tidsrammen er overskredet.

I saker hvor saksbehandlingstiden er så lang at det foreligger en krenkelse av EMK artikkel 6, vil konvensjonsbruddet måtte repareres etter EMK artikkel 13. For noen konvensjonsbrudd vil det kunne være tilstrekkelig reparasjon at krenkelsen konstateres i premissene for avgjørelsen, se f.eks. HR-2009-2179-A og HR-2012-132-U. Ved ileggelse av straff i straffelovens forstand kan reparasjon skje ved at det gis en reduksjon av straffen, men det kan også være aktuelt å gi betinget dom eller deldom, eller å velge en mildere straffart, jf. HR-2016-225-S avsnitt 39. Ved ileggelse av overtredelsesgebyr vil det mest praktiske som regel være å redusere gebyret.

Hvor stor reduksjonen skal være, vil bero på en konkret vurdering av en rekke forhold, blant annet saksbehandlingstidens lengde, sakens størrelse og kompleksitet og hva som er grunnen til at saksbehandlingen har tatt lang tid. Lang saksbehandlingstid vil kunne forsvares i store og komplekse saker, eller i saker hvor den behandlingsansvarlige selv kan lastes for den svake fremdriften. Omvendt vil perioder med liggetid – hvor det ikke gjøres noe med saken – som regel ikke kunne forsvares.

I straffesaker er det især perioder med ren liggetid som blir ansett for å utgjøre en krenkelse av EMK artikkel 6. I HR-2016-225-S ledet en liggetid på 7-8 måneder til en strafferabatt på ca. 12 prosent. I HR-2018-1987-A ga en liggetid på 1,5 år en strafferabatt på ca. 19 prosent. I HR-2022-1319-A ledet en liggetid på 1 år og 9 måneder til en strafferabatt på 33 prosent. I Rt-2014-666 ledet en liggetid på 2,5 år til en strafferabatt på 20 prosent, mens det i HR-2017-1072-A ble gitt en strafferabatt på hele 44 prosent. Tallene gir en indikasjon på hvor nivået ligger, men viser samtidig at utmålingen i hver enkelt sak vil bero på et konkret skjønn.

I skatteforvaltningen – som er et område som i utpreget grad utgjør masseforvaltning – er det fastsatt nærmere regler om utmålingen ved konvensjonsbrudd i skatteforvaltningsforskriften § 14-12-1 første ledd. Bestemmelsen lyder slik:

> «Når det foreligger brudd på kravet om avgjørelse innen rimelig tid, gis kompensasjon med halvannet rettsgebyr per påbegynte måned fra varsel om tilleggsskatt eller overtredelsesgebyr er sendt, til saken er avgjort.»

Rettsgebyret er for tiden 1 314 kroner, jf. rettsgebyrforskriften § 2-1. Dette innebærer at reduksjonen blir 1 971 kroner per måned – og 23 652 kroner per år.

Nemnda har vurdert om det kan være grunn til å legge et tilsvarende utgangspunkt til grunn ved utmåling av overtredelsesgebyr i tilfeller hvor det foreligger konvensjonsbrudd. Nemnda har imidlertid blitt stående ved at denne ordningen legger for sterke bånd på utmålingen, siden den i liten grad gir rom for å foreta konkrete vurderinger. I tilfeller hvor overtredelsesgebyret er høyt, er det dessuten et spørsmål om ordningen gir tilstrekkelig reparasjon. Etter nemndas syn er det derfor grunn til å holde fast ved at utmålingen bør bero på et konkret skjønn.

I nemndas praksis finnes det flere eksempler på at lang saksbehandlingstid har ledet til en betydelig reduksjon av overtredelsesgebyret, og det finnes også saker hvor gebyret har falt helt bort. Denne praksisen går atskillig lenger enn det som kreves etter EMK artikkel 13, og den vil ikke bli videreført. Nemnda vil i stedet legge seg på en praksis som speiler Norges forpliktelser etter konvensjonen – og hvor det dessuten tas hensyn til de forventninger som springer ut av kravene til saksbehandlingstidens lengde etter forvaltningsloven § 11 a. Dette innebærer en viss innstramming av praksis sammenholdt med tidligere. Forbudet mot usaklig forskjellsbehandling er imidlertid ikke til hinder for å legge om praksis innenfor rammene av skjønnsfriheten, jf. Rt-2006-564 avsnitt 40 og Rt-2012-1444 avsnitt 56 og 57.

Etter nemndas syn gir den praksis Høyesterett som følger i straffesaker, en viss veiledning også i saker om utmåling av overtredelsesgebyr etter personopplysningsloven. Nemnda vil derfor legge seg på en praksis hvor det i normaltilfellene gis en gebyrreduksjon på mellom 0–10 prosent i saker hvor liggetiden er opptil 1 år. Dersom liggetiden er mellom 1–2 år, vil reduksjonen i normaltilfellene være mellom 10–20 prosent. Dersom liggetiden er mellom 2–3 år, vil reduksjonen i normaltilfellene være mellom 20–30 prosent. Dersom liggetiden er mellom 3–5 år, vil reduksjonen i normaltilfellene være mellom 30–50 prosent. Er liggetiden helt unntaksvis enda lengre, vil det kunne være aktuelt med en større reduksjon. Det er grunn til å understreke at dette utelukkende skal anses som veiledende utgangspunkter for utmålingen. I en konkret sak vil reduksjonen kunne bli høyere og lavere enn det disse angivelsene tilsier – alt etter hva som er nødvendig for å reparere krenkelsen, jf. EMK artikkel 13. Det vil i tillegg kunne tas hensyn til omfanget av bruddet på forvaltningsloven § 11 a første ledd, som krever av saken må forberedes og avgjøres uten ugrunnet opphold.

I den foreliggende sak antar nemnda at den samlede liggetiden er nærmere tre år. Datatilsynet reduserte det opprinnelige overtredelsesgebyret med 1 000 000 kroner, som utgjør en reduksjon på 40 prosent. Etter nemndas syn er denne reduksjonen i tråd med de veiledende utgangspunkter som er oppstilt ovenfor, og nemnda er enig i den endelige utmålingen.

Klagen tas ikke til følge.

Vedtaket er enstemmig.

**5. Konklusjon**
Datatilsynets omgjøringsvedtak 2. april 2025 stadfestes.

Marius Stub
leder

Dette brevet er godkjent elektronisk og har derfor ikke håndskrevet underskrift.